ERROR CORRECTING CODING SCHEME AGAINST PARTIAL TIME JAMMERS

Philippe Sadot, Marc Darmon

ALCATEL THOMSON FAISCEAUX HERTZIENS
55, rue Greffülhe, 92301 - LEVALLOIS-PERRET

Résumé :

Cet article propose une approche nouvelle de la lutte contre les brouilleurs impulsionnels de forte puissance, pour les applications où le schéma classique étalement de spectre + codage correcteur d'erreurs n'est pas efficace du fait de la trop faible valeur du gain d'étalement. Son principe est d'admettre que toutes les informations utiles sont effacées pendant les impulsions du brouilleur, et d'exploiter la brièveté de ces impulsions pour essayer de reconstituer l'information perdue au moyen de codes correcteurs d'erreurs et d'effacements. Pour que le système résiste aux brouilleurs "intelligents", une technique nouvelle d'entrelacement pseudo-aléatoire est proposée ; un schéma de codage efficace est décrit, et une nouvelle méthode de localisation des effacements est proposée.

Summary :

This paper proposes a new approach to antijamming against high energy partial time jammers concerning applications where the usual scheme sprectrum spreading + error correcting coding is not efficient because of the small value of the spreading gain, due to the channel bandwith limitation and to the minimum data rate required on the link. It consists in exploiting the short duration of the jamming pulses and trying to reconstitute the erased information by means of error correcting codes. A new method of pseudorandom interleaving, an efficient coding scheme, and a new method of erasure localization are proposed.

Introduction

The traditional means of antijamming on the digital links consist in the use of spread spectrum techniques, by direct sequence or by frequency hopping, in association with error correcting coding. The aim of the spectrum spreading is to break up the energy of the jammer into a frequency band much wider than the signal band ; the role of the correcting codes is to compensate the BER degradation owed to the jammer's residual energy in the signal's band. To be efficient these techniques require a large spreading gain (typically > 20 dB) ; in the case of microwave links, it seems difficult to obtain such a value : the data rate can't be lower than a minimum value under which the link has no operational interest anylonger (256 kbps for instance), and the spreading bandwidth is limited by the channel bandwidth. For instance, spreading of a signal at 256 kbit/s into a band of 34 MHz provides a gain of 21 dB, and this seems to be an absolute maximum. Therefore the usual scheme spreading + coding can't be efficient in a set of situations concerning the microwave links, where the J/S ratio of the jammer's power to the signal's power is greater than the receiver's jamming margin. This is particularly the case of the pulse jammers that are able to concentrate a tremendous power during very short lapses of time. In such a situation the approach of the antijamming strategy has to be completely reconsidered : if it is not possible to cast off the jammer, it is on the other hand possible to take advantage of the short duration of its pulses. The principle is to admit that all information is erased during the pulses and then to try to reconstitute the lost information by means of error correcting codes used in erasure correction. In the following we explain the choice of the coding scheme, and propose possible means to localize erasures in the digital stream.

Nature of the perturbations

As we already said, the jammer's activity causes erasure bursts we can characterize by their duration and their mean recurrence. The orders we took for these parameters are the following :

- pulse duration : about 2 ms,
- max recurrence : up to 1/10. (The jammer may be non periodic.)

Of course the links are also perturbed by thermal noise that the codes have to take into account.

Necessity of interleaving

A 2 ms pulse on an 8 Mbps link causes the erasing of 16000 symbols : the use of an interleaving device is indispensable. Among the different kinds of interleaving the most convenient is the pseudo-random interleaver, which permits to combat "intelligent" jammers, capable of adjusting the duration and the recurrence of their pulses to the structure of a periodic interleaver, in order to create error bursts in the digital stream after de-interleaving. We have defined a pseudo-random interleaver combining the advantages of the periodic interleaving (large minimal distance,[1]) and of the fully random interleaving (unpredictability of the sent out symbols order). It uses a matrix which is read and written at the same address. These addresses are given by a 'driving sequence' : the symbol which is located at the address given by the driving sequence in the register is sent out and replaced by

the next symbol to be transmitted ; deinterleaving is achieved in the same way. Obviously, the interleaving quality (minimal distance) and the resistance to intelligent jammers depend on the driving sequence : it has been built from a high linear complexity pseudo random sequence [2] and a set of three rules insuring a good interleaving quality.
Two patents have been registered in Europe about this interleaving system [3,4].

Obtaining the driving sequence :

The driving sequence is the sequence of addresses where the interleaving register has to be read and filled. Let **d** be the aimed minimal distance of the interleaver. To obtain an address, we choose among the addresses given by the high linear complexity random generator the ones which verify the three following rules:
[1] All addresses must have been selected before reselecting one of them. Already chosen addresses have a 'permanent banning' until the end of the register.
[2] When a symbol has been sent out, no other symbols of the same codeword should be transmitted during (d-1) selections. Addresses where the other symbols of the same codeword are, have a temporary banning during (d-1) address selections.
[3] If there is a deadlock (i.e. no address can be chosen without infringing rules 1 or 2), any address which does not go against the first rule can be chosen.

Deinterleaving :

Deinterleaving is achieved in the same way, using a receiver register, which is read and written at the addresses given by an 'inverse driving sequence' (IDS). The receiver register has the same size as the interleaving register. The inverse driving sequence is obtained from the driving sequence [4].

Register size :

For a periodic interleaver, the matrix size that guarantees a minimal distance **d** after interleaving between two symbols of the same **Lc** symbol long code word, is **M=Lc*d**. The size of our pseudorandom interleaving register is **M=Lc*(d+1)** ; we have to use occasionally the third rule and the distances between two symbols of the same codeword may be sometimes smaller than **d**. We observed that it seldom occurs, and minimal distance is only slightly smaller than **d**. The register has only to be oversized with regard to the jammer pulses length.

A pseudo-random generator :

In order to obtain the driving sequences, we need a pseudo-random generator. To resist against an intelligent jammer, we have to use a cryptographic quality pseudo-random generator. For that we used some results about Galois Fields and linear complexity given by Rueppel [2]. In particular, a non-linear function of the output sequences of any N maximum-length LFSRs (started in a non-zero state) of different lengths (greater than 2) will produce a binary sequence whose complexity is maximum, i.e. is equal to the product of the complexities (the lengths) of the LFSRs : this means that an attempt to synthetize the produced sequence by means of a single LFSR would require a LFSR of length equal to the product of the lengths of the LFSRs, and this number may easily reach a few thousands. And even if the structure of the generator is known, its number of possible initializations is equal to $(2^{L1}-1)...(2^{LN}-1)$, where Li is the length of register i, 1<=i<=N, and may be easily as great as 2^{150}, which guarantees the cryptographic solidity of the generator.

Choice of a non binary code

A characteristic we have to take advantage of is the burst structure of the erasures caused by a jammer. This leads to use a non binary code, i. e. a code working on m-bit symbols, for which a symbol is erased as soon as one of its bits is. The erasures being grouped, it is likely that all the bits of an erased symbol will be erased : this means that a non-binary code will see m times less erasures than a binary one. Among the non binary codes that can be decoded in erasure mode is the family of the Reed-Solomon codes, which are optimal since they are maximum distance separable.

Interest of a concatenated scheme

The implementation of a powerful high data rate (8 Mbps) of a Reed-Solomon code is a difficult and onerous operation. What is more, the use of just one code is not very efficient against thermal noise and erasures : a RS (n,k) code is indeed able to correct any configuration of ν errors and σ erasures provided that $2\nu + \sigma < n - k + 1$: the presence of one error diminuates the erasure correction capability of 2 units. To obviate this problem, it is possible to separate the tasks of error and erasure correction between two concatenated codes : a simple internal error correcting code and an erasure correcting Reed-Solomon code. The scheme can be improved if we notice that it is possible to use also the internal code in erasure correction when there is no errors. In a concatenated scheme the Reed-Solomon code has to be much less powerful than if he were alone ; hence, its implementation is much simpler and cost effective. After some calculations and simulations, we have shown that the association of an external (15,8) Reed-Solomon code and of an internal (7,4) Hamming code, both decoded in error and erasure correction, was able to correct more errors and erasures than a single (31,15) Reed-Solomon code whose realization is about four times more complex. In order to have a coding rate of the form 2^{-r}, which was more convenient in our applications, we have withhold the following scheme :
External shortened (14,7) RS code + internal extended (8,4) Hamming code + pseudo-random interleaving
The calculation of its performances gives the curves of figure 1. On this figure the x-axis gives the error probability on the channel due to thermal noise, the curves are parametered by the max erasure rate of the jammer, i. e. its maximum recurrence, and the y-axis gives the residual binary error rate after decoding.One can see that for an erasure rate equal to 1/4 and an error probability equal to 10^{-4}, the residual binary error rate is about 10^{-6}.

Localization of the erasures

This system works well provided we are able to localize the erasures in the digital stream with a rather good accuracy. Several solutions may be considered :
- **using external informations,** such as the loop voltage of the automatic gain control amplifier (AGC),the eye level at the output

of the demodulator ; when a jammer is active the AGC indicates a high received power while the eye level is very poor,

- **using the internal code,** whose distance is 4, and which is also able to detect two errors and correct one. Each time the code detects two errors is declares the correspondent word as erased and then integrates this information along the received sequence. This method has two major drawbacks :

the integration along the interleaved sequence cause an important delay,

the internal code is not used as erasure corrector, this diminuates ly the correction capability of the concanated scheme,

- **using an other internal code,** located after the interleaver and also not protected by it.

The principle is the following :

- when the link is not affected by a jammer, the BER is better than 10^{-5} for instance. The third code has nothing to do in this situation, i. e. the probability **Pf** the code fails to decode must be arbitrarily small.

- during the pulses the BER becomes very high, in any case worse than a given value, 5.10-2 for instance ; we will choose the code so that its correction probability **Pc** in this case is arbitrarily small. If the code used is linear it is easy to verify if the corrected word really belongs to the code (good decoding) or not (bad decoding) by simple calculation of the syndromes of the corrected word. If a sequence of consecutive words is badly decoded, we can be sure that the link is jammed because the code has been chosen so that the probability of this event on a jammer free channel is extremely small. Of course, this can only work if the code used has a low covering radius t. If we used a perfect code all the received words could be decodable and this system would be of no use. If we assume that the jammer is so strong that all the n-bit words have the same probability at the receiving end (BER = 0.5), the probability of a correctable received word, i. e. of non detection of the erasure, is equal to the covering radius of the code. The characteristics of this internal code should be also the following :

- high coding rate (>0.8 for instance), in order not to modify the conditions of the link,
- low covering radius τ,
- $Pf < \varepsilon$ (ε arbitrarily small)
- $Pc < \varepsilon$

Interesting codes can be found among the long BCH codes (255, 511, 1023) : the high rate long BCH codes satisfy the above conditions except the low covering radius one ; it is possible to reduce artificially the radius of the decoding spheres by underexploiting the correction capability of the code. An other is to integrate the erasure detection information by means of an up/down counter with saturation at a level q, and to decide that the received words are erased as long as the output of the counter is different of zero. This avoids a word to be badly decoded among a sequence of erased words, which might lead the following interleaving and coding devices astray : the probability of this event becomes equal to τ^q. Of course, this has the drawback of artificially lengthening the pulse duration, as the **q-1** words incoming after the end of the jammer pulse are still considered as erased. In fact, a numerical example shows that it is not awkward. Assume for instance that the error rate on the channel is $p = 10^{-5}$ when the jammer is not active and $p = 10^{-2}$ when it is. Let's choose $\varepsilon = 10^{-6}$. If we use a BCH (255,215,5) code, we get $Pf = 3.10^{-19}$, $Pc = 3.8\ 10^{-7}$, $\tau = 10^{-2}$. As τ seems too large, we can use an up/down counter with saturation level $q = 3$, so that the probability of non detection becomes $\tau^3 = 10^{-6}$. For a data rate of 2.340 Mbps, the on-line rate is equal to 2.340 x 255 / 215 = 2.775 Mbps ; if the pulse duration is 5 ms, 13875 bits ,i. e. 13875 / 255 = 55 words, are erased. Because of the use of counter by 3, 2 more words will be declared erased, which is not penalizing. This erasure detection method has been patented [5].

Conclusion

We have explained in this paper a new approach to antijamming against high energy pulse jammers using only error and erasure correcting codes, but no techniques of spectrum spreading as it is usual.

The performance of the proposed coding and interleaving scheme are excellent since it permits to insure the reliability of the link even against a jammer that would erase all information during 25 % of the time, the link being affected by thermal noise generating a BER of 10^{-4}. Even if, by now, high power jammers may not be able to produce such an erasure rate, this performance allows a good reliability when several less recurrent jammers are threatening the link.

References

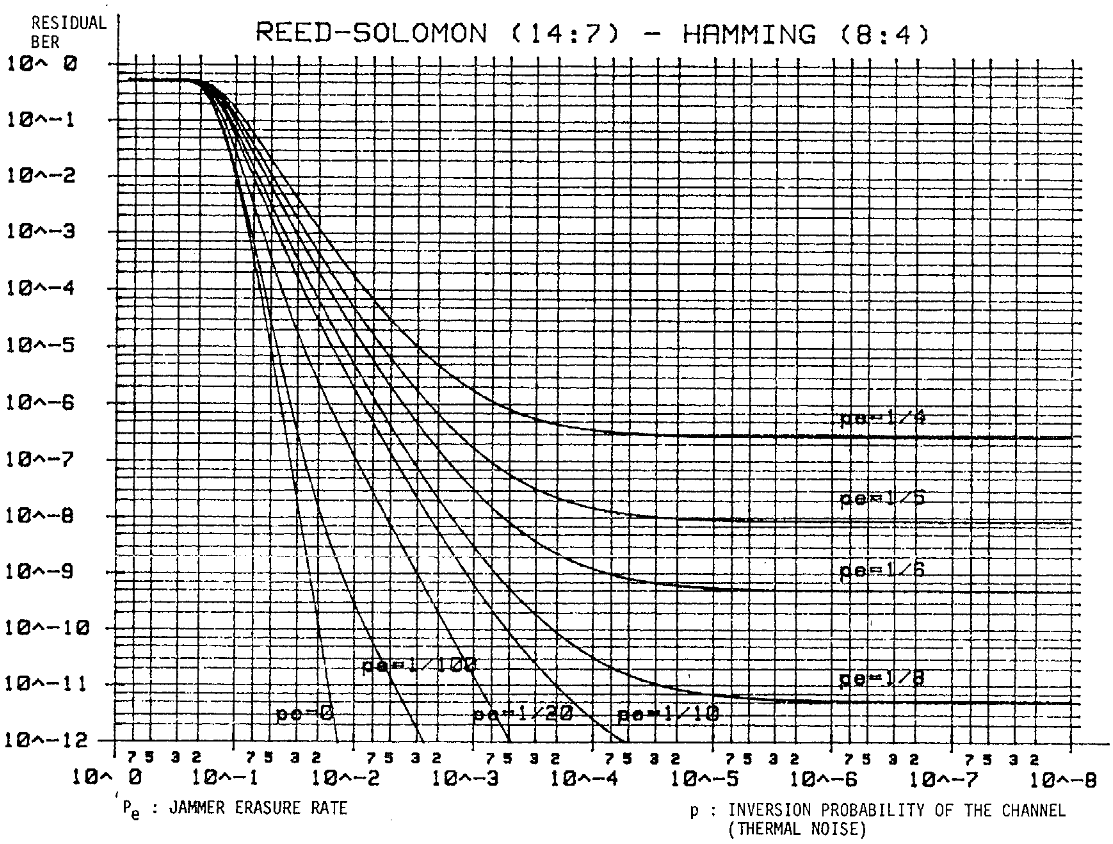
[1] Ramsey J. L., Realization of optimal interleavers, IEEE Trans. on IT, May 1970, #3

[2] Rueppel R. A., Analysis and design of stream cyphers, Springer Verlag

[3] Sadot Ph., Darmon M., European patent # 88.15421

[4] Darmon M., Sadot Ph., European patent # 88.15422

[5] Sadot Ph., European patent # 87.17645



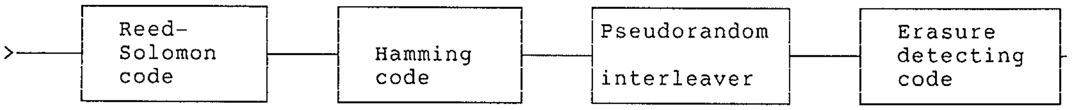
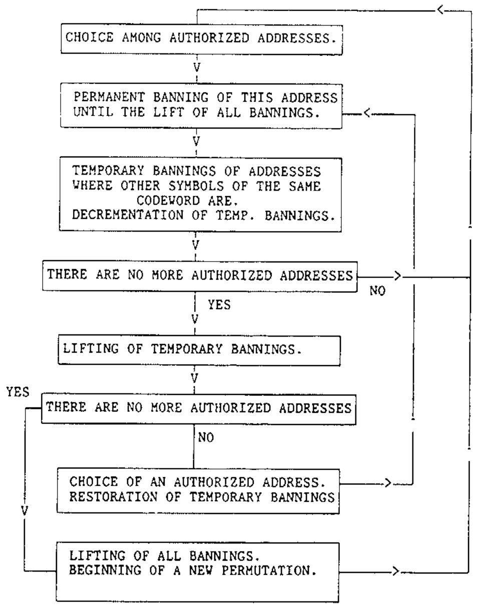


Fig_2 : Insertion of a third code for erasure detection

PSEUDO-RANDOM INTERLEAVING : DRIVING SEQUENCE OBTAINING ALGORITHM


CHOICE AMONG AUTHORIZED ADDRESSES.
PERMANENT BANNING OF THIS ADDRESS UNTIL THE LIFT OF ALL BANNINGS.
TEMPORARY BANNINGS OF ADDRESSES WHERE OTHER SYMBOLS OF THE SAME CODEWORD ARE. DECREMENTATION OF TEMP. BANNINGS.
THERE ARE NO MORE AUTHORIZED ADDRESSES
NO
YES
LIFTING OF TEMPORARY BANNINGS.
YES
THERE ARE NO MORE AUTHORIZED ADDRESSES
NO
CHOICE OF AN AUTHORIZED ADDRESS. RESTORATION OF TEMPORARY BANNINGS
LIFTING OF ALL BANNINGS. BEGINNING OF A NEW PERMUTATION.